CLAIMS

What is claimed is:

1. A method of secure session management and authentication between a web site and a web client, said web site having secure and non-secure web pages, said method comprising the steps of:

a) utilizing a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages; and

b) utilizing a secure communication protocol and an authcode cookie when said web client requests access to said secure web pages.

2. The method of claim 1, wherein said method also comprises the steps of:

c) requesting said session cookie from said web client when said web client requests access to said non-secure web pages and verifying said requested session cookie; and

d) requesting said authcode cookie from said web client when said web client requests access to said secure web pages and verifying said requested authcode cookie.

3. The method of claim 2, wherein said method also comprises alternating between said secure communication protocol and said non-secure communication protocol when said web client alternates requests for access to said secure web pages and said non-secure web pages.

4. The method of claim 3, wherein said alternating between said secure communication protocol and said non-secure communication protocol is facilitated by a table which keeps track of said non-secure web pages and said secure web pages.

5. The method of claim 4, wherein said web site uses said table to direct said web client to use said secure communication protocol or said non-secure communication protocol depending on whether said web client requests access to said non-secure web pages or said secure web pages.

6. The method of claim 3, wherein said method also comprises allowing said web client to be

a guest client or a registered client.

7. The method of claim 6, wherein said method also comprises creating stored information including data contained in said session cookie, data contained in said authcode cookie and data about said web client.

8. The method of claim 7, wherein said session cookie includes a pointer and an encrypted portion, said pointer pointing to said stored information, said encrypted portion having a random portion and a date portion.

9. The method of claim 7, wherein said authcode cookie includes an encrypted portion, said encrypted portion having a random portion and a date portion.

10. The method of claim 8, wherein verifying said requested session cookie from said web client includes using said stored information to generate a second session cookie and comparing said second session cookie to said session cookie requested from said web client.

11. The method of claim 9, wherein verifying said requested authcode cookie from said web client includes using said stored information to generate a second authcode cookie and comparing said second authcode cookie to said authcode cookie requested from said web client.

12. A system, for secure session management and authentication between a web site and a web client, said system comprising a web server, a web client and a communication channel, said web server coupled to said web client via said communication channel, said web server having a web site, said web site including:

a) secure and non-secure web pages;

b) a non-secure communication protocol and a session cookie for allowing said web client access to said non-secure web pages; and

c) a secure communication protocol and an authcode cookie for allowing said web

client access to said secure web pages.

13. The system of claim 12, wherein said web site also includes:

d) verification means for verifying said session cookie when said session cookie is requested from said web client; and

e) verification means for verifying said authcode cookie when said authcode cookie is requested from said web client.

14. The system of claim 13, wherein said web server further comprises a security alternating means for alternating between said secure communication protocol and said non-secure communication protocol.

15. The system of claim 14, wherein said web server further comprises a table to keep track of said non-secure web pages and said secure web pages.

16. The system of claim 13, wherein said web site includes access means to allow said web client to access said web site as a guest client or a registered client.

17. The system of claim 16, wherein said web system has storage means for containing stored information about said web client, data contained in said session cookie and data contained in said authcode cookie.

18. The system of claim 17, wherein said session cookie includes a pointer and an encrypted portion, said pointer pointing to said stored information, said encrypted portion having a random portion and a date portion.

19. The system of claim 17, wherein said authcode cookie includes an encrypted portion, said encrypted portion having a random portion and a date portion.

20. A computer program embodied on a computer readable medium, said computer program providing for secure session management and authentication between a web site and a web client, said web site having secure and non-secure web pages, said computer program adapted to:

a) use a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages; and

b) use a secure communication protocol and an authcode cookie when said web client requests access to said secure web pages.

21. The computer program of claim 20, wherein said computer program is further adapted to:

c) request said session cookie from said web client when said web client requests access to said non-secure web pages and to verify said requested session cookie; and

d) request said authcode cookie from said web client when said web client requests access to said secure web pages and to verify said requested authcode cookie.

22. The computer program of claim 21, wherein said computer program is further adapted to alternate between said secure communication protocol and said non-secure communication protocol when said web client alternates requests for access to said secure web pages and said non-secure web pages.

23. The computer program of claim 22, wherein said alternating between said secure communication protocol and said non-secure communication protocol is facilitated by a table which keeps track of said non-secure web pages and said secure web pages.

24. The computer program of claim 23, wherein said computer program uses said table to direct said web client to use said secure communication protocol or said non-secure communication protocol depending on whether said web client requests access to said non-secure web pages or said secure web pages.

25. The computer program of claim 22, wherein said computer program is adapted to allow said

web client to be a guest client or a registered client.

26. The computer program of claim 25, wherein said computer program is adapted to create stored information including data contained in said session cookie, data contained in said authcode cookie and data about said web client.

27. The computer program of claim 26, wherein said session cookie includes a pointer and an encrypted portion, said pointer pointing to said stored information, said encrypted portion having a random portion and a date portion.

28. The computer program of claim 26, wherein said authcode cookie includes an encrypted portion, said encrypted portion having a random portion and a date portion.

29. The computer program of claim 27, wherein verifying said requested session cookie from said web client includes using said stored information to generate a second session cookie and comparing said second session cookie to said session cookie requested from said web client.

30. The computer program of claim 28, wherein verifying said requested authcode cookie from said web client includes using said stored information to generate a second authcode cookie and comparing said second authcode cookie to said authcode cookie requested from said web client.

31. A computer program for creating a NAME attribute in a session cookie, said computer program comprising the steps of:

a) generating a user_id;

b) generating a session_string;

c) generating a session_timestamp;

d) appending said session_timestamp to said session_string to create an intermediate

value;

e) applying a one way hash function to said intermediate value to create a final value; and

f) storing said final value in said NAME attribute.

32. The computer program of claim 31, wherein creating a PATH attribute, an EXPIRES attribute, a DOMAIN attribute and a SECURE attribute in said session cookie comprises the steps of:

a) storing a slash (Ò/Ó) in said PATH attribute;

b) storing a null string (ÒÓ) in said EXPIRES attribute;

c) storing a null string (ÒÓ) in said DOMAIN attribute; and

d) storing a null string (ÒÓ) in said SECURE attribute.

33. A computer program for creating a NAME attribute in an authcode cookie, said computer program comprising the steps of:

a) generating an authcode;

b) generating an authcode_timestamp;

c) appending said authcode_timestamp to said authcode to create an intermediate value;

d) applying a one way hash function to said intermediate value to create a final value; and

e) storing said final value in said NAME attribute.

34. The computer program of claim 33, wherein creating a PATH attribute, an EXPIRES attribute, a DOMAIN attribute and a SECURE attribute in said authcode cookie comprises the steps of:

a) storing a slash (Ò/Ó) in said PATH attribute;

b) storing a null string (ÒÓ) in said EXPIRES attribute;

c) storing a null string (ÒÓ) in said DOMAIN attribute; and

d) storing the string ÒsecureÓ in said SECURE attribute.